ABSTRACT

A system for increasing transaction security across existing infrastructure is provided. An activation mechanism sends an activation signal or a signal providing a PIN and/or other data to a processing device. If the data is verifiable, the processing device performs verification. A display unit provides a key, preferably encrypted, upon successful utilization of the sensor device. Included in the key generation mechanism is an indicator of the transaction number or other sequential count indicative of card use. An authorization service reads the key from a transaction communication PIN field and decrypts based on a second sequential count maintained in sync with the first count to determine whether the use is authorized. In one embodiment a clocking mechanism is also utilized in encrypting and decrypting the key. A separate reader may be similarly configured to read existing smart cards utilizing the process of the present invention.